IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF OHIO
EASTERN DIVISION

UNITED STATES OF AMERICA,	)	CASE NO.: 5:18-CR-448
	)	
Plaintiff,	)	JUDGE BENITA Y. PEARSON
	)	
v.	)	
	)	
PHILIP M. POPA, JR.,	)	UNITED STATES' OMNIBUS
	)	RESPONSE IN OPPOSITION TO
Defendant.	)	DEFENDANT'S MOTION TO
	)	COMPEL [R. 23] AND MOTION TO
	)	SUPPRESS [R. 24]

I. SUMMARY OF THE GOVERNMENT'S RESPONSE

A. THE MOTION TO COMPEL

The government writes in opposition to the motion by defendant Popa seeking to compel the production of the law enforcement software utilized by Officer Anschutz in his investigation of Freenet. Popa further demands that the government either provide the law enforcement software to the not-yet retained defense forensic examiner, Tami Loehrs, for testing and evaluation or, in the alternative, documentation of testing and validation of the law enforcement software by a qualified third party. (R. 23: Motion to Compel, PageID 79). In short, the defendant contends that his examiner requires a copy of this law enforcement sensitive investigatory program – which detected a Freenet user (later identified as Popa) requesting pieces of a known child pornography file – for three purported reasons: to assess the reliability and functionality of the Freenet software; to assess pretrial motions; and to effectively cross examine Agent Anschutz. (Id.).

Consistent with the Sixth Circuit's opinion in United States v. Pirosko, 787 F.3d 358 (6th Cir. 2015), the defendant has failed to demonstrate a need to expose the law enforcement tool or establish materiality. As shown below, the defendant's motion rest on the erroneous assertions of his "expert," Tami Loehrs, who travels around the country making similar fantastic claims in child pornography cases in an effort to further her forensic computer business. The government believes that Ms. Loehrs is seeking production of the sensitive law enforcement program at issue, as she has done in other cases, simply to make herself more marketable in the child pornography defense realm. The vague assertions of Ms. Loehrs in support of this motion should be treated with caution, given her history of supporting comparable motions which have been found by other courts to be misleading and/or flawed.

B. THE MOTION TO SUPPRESS

On February 11, 2019, Popa filed the instant Motion to Suppress evidence obtained as a result of the execution of a federal search warrant at his residence. He alleges that obtaining his IP address through an administrative subpoena violated Carpenter v. United States, 138 S. Ct. 2206, 201 L.Ed.2d 507 (2018). Carpenter did not address the requirements to obtain basic subscriber information pursuant to 18 U.S.C. § 2703(c)(2) and is inapplicable here.

Second, the residential search warrant was amply supported by probable cause to believe that Popa had requested child pornography files through the peer-to-peer network and, accordingly, that evidence of child pornography crimes would be located at his residence.

Finally, even if the warrant were found to be deficient, law enforcement reasonably relied upon its issuance by a neutral and detached magistrate and the Leon good faith exception applies to bar suppression of evidence. Accordingly, the motion to suppress evidence should be denied.

II. FACTUAL SUMMARY

A. HISTORY OF THE CASE

In or around April of 2018, FBI TFO Ryan Anschutz was operating undercover on an Internet-based, peer-to-peer (P2P) network known as "Freenet". (R. 23-1: Application for a Search Warrant, Page ID 96).[1] Freenet allows users to anonymously share files, chat on message boards, and access websites within the network. (Id. PageID 87). TFO Anschutz reviewed information obtained and logged by law enforcement Freenet computers that showed a Freenet user with IP address 173.90.126.69 requested pieces of child pornography files. TFO Anschutz concluded that the user of IP address 173.90.126.69 was the original requestor of each of the files. (Id. PageID 95-96).

More specifically, On April 21, 2018, between 8:52 AM UTC and 10:20 AM UTC, a computer running Freenet software, with an IP address of 173.90.126.69, *with 13.1 peers*, requested from a law enforcement computer 136 out of 1786 total pieces needed to assemble a file with a SHA1 digital hash value of ATLOOVASIDQV6JPN****************[2]. TFO Anschutz downloaded the exact same file with the above referenced SHA1 hash value from Freenet and found a folder titled "Alena 3yo an dDad (2014).7z. Once the folder was expanded 69 color pictures were observed, 54 of which depict a prepubescent child exposing her genitalia

[1] A complete copy of the Application for a Search Warrant for 533 Redwood St SW, including TFO Ryan Anschutz's affidavit, signed by Magistrate Judge George J. Limbert was included as an exhibit to Popa's Motion to Compel. (R. 23-1). The exhibit was sealed since the original search warrant was filed under seal. Therefore, the Government will refer to the previously filed and sealed copy of the Application herein.

[2] Half of the actual hash values listed in the original affidavit have been redacted to avoid disseminating this information to the public.

and an adult male hand spreading her genitalia apart for the focal point of the camera. (Emphasis added) (Id. PageID 96).

In addition, on April 21, 2018, between 9:03 AM UTC and 10:04 AM UTC, a computer running Freenet software, with the same IP address of 173.90.126.69, *with 13 peers*, requested from a law enforcement computer 43 out of 685 total pieces needed to assemble a file with a SHA1 digital hash value of YMHVDJCZSZ4CD6F3****************. TFO Anschutz downloaded the exact same file with the above referenced SHA1 hash value from Freenet and found it to contain a 5 minute 43 second color video of a prepubescent toddler female laying on her back on a mattress with a masked adult female next to her. The toddler can be heard crying as the adult female removes her diaper and rubs ice cubes all over the body and genitalia of the toddler. The adult then binds the toddler's feet with rope to a wooden rod and hangs the toddler upside down. She duct tapes the toddlers hands and mouth. The female then strikes the toddlers exposed genitalia, puts clothespins on the toddlers exposed nipples and genitalia, and then drips hot wax on the toddler's exposed genitalia. (Emphasis added) (Id. PageID 96-97).

Further, on April 21, 2018, between 9:15 AM UTC and 10:06 AM UTC, a computer running Freenet software, with the same IP address of 173.90.126.69, *with 13.0 peers*, requested from a law enforcement computer 49 out of 633 total pieces needed to assemble a file with a SHA1 digital hash value of IW4WRTR2ALAEQFD2****************. TFO Anschutz downloaded the exact same file with the above referenced SHA1 hash value from Freenet and found a color video of a prepubescent toddler female that is approximately 9 minutes 40 seconds in length. Throughout the video the naked toddler is observed with her ankles bound by rope to a wooden rod; hung upside down above a mattress and forced to put her mouth on an adult breast and adult female genitalia; her arms are duct taped behind her back and her mouth taped; she is vaginally raped with an object and beat with a leather strap; and is burned with a candle and dripping wax. (Emphasis added) (Id. PageID 97-98).

On June 1, 2018, TFO Anschutz queried the IP address 173.90.126.69 through the American Registry for Internet Numbers ("ARIN"), a publicly available search tool, which reported that this IP address was registered to Time Warner Cable. (Id. PageID 99). An administrative subpoena was sent to Time Warner Cable and law enforcement learned that on the date and times in question, the IP address was registered to "James Skelly," in Beach City, Ohio. (Id.) On July 17, 2018, a federal search warrant was issued for this residence.

On July 17, 2018, a federal search warrant was executed at Popa's residence in Beach City, Ohio. During an interview with law enforcement, Popa ultimately admitted to using Freenet to view and download child pornography on his HP laptop computer. (R. 1: Criminal Complaint, ¶13, filed under seal). Popa described downloading a file of an infant being abused and "something with an ice cube." (Id.) This file with the SHA1 digital hash value of YMHVDJCZSZ4CD6F3*************** was located during a forensic preview of his laptop computer. It is identical by hash value and content to the image described above from the Application. (Id., ¶14).

On July 19, 2018, a Criminal Complaint was signed by Magistrate Judge George J. Limbert. (R. 1: Criminal Complaint, PageID 1). This was followed by an Indictment returned on August 14, 2018, charging Popa with one count of Receipt of Visual Depictions of Real Minors Engaged in Sexually Explicit Conduct, in violation of 18 U.S.C. §2252(a)(2), and one count of Possession of Child Pornography, in violation of 18 U.S.C. §2252A(a)(5)(B). (R. 11: Indictment, PageID 23-24).

On January 29, 2019, defense counsel requested and the government provided a copy of the academic paper referred to in the warrant. The government refused to turn over the law enforcement software requested that same day. (See Attachment D: Email communication with defense counsel dated 1/29/19).

On February 11, 2109, Popa filed three motions with this Court. The first being a Motion to Compel, seeking the Freenet log files from Popa's case[3], an installable copy of the Freenet software used by TFO Anschutz for testing and validation; and a forensic image of all electronic evidence seized from Popa to be sent to the FBI facility in Arizona.[4] (R. 23: Motion to Compel, PageID 68-80). Attached to this request was a copy of the Sealed Application for a Search Warrant signed by Magistrate Judge George J. Limbert on July 17, 2018. (R. 23-1: Application, PageID 81-121, sealed). Also attached was an 8 page affidavit from Tami Loehrs and an 18 page Curriculum Vitae for Ms. Loehrs. (R. 23-2: Loehrs affidavit, PageID 122-146).

Popa filed a contemporaneous Motion to Suppress and Motion to Supplement alleging the government obtained account information for his Internet Protocol ("IP") address in violation of Carpenter v. United States, 138 S. Ct. 2206, 201 L.Ed.2d 507 (2018) (holding that the Government must get a warrant before acquiring cell-site location information from a wireless carrier). Further, Popa alleges a violation of Franks v. Delaware, 438 U.S. 154 (1978), arguing that TFO Anschutz claimed he relied on a peer-reviewed article but that fact does not appear to be true. (R. 24: Motion to Suppress, PageID 148-160). Attached to this motion is a copy of the

[3] This was the first request by the defense for the Freenet log files. The files were provided to defense counsel on February 19, 2019. (See Attachment E: Email communication with defense counsel dated 2/19/19)

[4] Presumably this request is for the convenience of Tami Loehrs, whose company, Loehrs Forensics, LLC, is located in Tucson, Arizona.

Application for a Search Warrant (R. 24-1: Application, PageID), the Loehrs affidavit and curriculum vitae. (R. 24-2: Affidavit and CV of Loehrs, PageID 202-227), and a portion of an article located on the freenetproject.org website titled Police Department's Tracking Efforts Based on False Statistics, dated May 26, 2016. (R. 24-3: Freenet article, PageID 228-230).

Finally, Popa filed a Motion to Appoint Expert, requesting that Tami Loehrs be appointed as an expert in this matter to assist defense counsel in understanding and addressing the digital forensics at the heart of this case and to conduct a forensic examination of the evidence. (R. 25: Motion to Appoint Expert, PageID 231-233). This was also accompanied by the Loehrs affidavit and curriculum vitae. (R. 25-1: Affidavit and CV of Loehrs, PageID 234-258).

B. DESCRIPTION OF FREENET AND THE MODIFIED LAW ENFORCEMENT VERSION OF FREENET

Peer-to-Peer ("P2P") file sharing networks allow their users to share and receive electronic files, including images, and videos, with a network of other users. To exchange files, users' computers communicate directly with each other, rather than through central servers. See Metro–Goldwyn–Mayer Studios Inc. v. Grokster, Ltd., 545 U.S. 913, 919–20 (2005). Freenet is an example of one such network. TFO Anschutz's affidavit in support of the residential search warrant (hereafter "the Affidavit") explained at great length how Freenet works and how law enforcement investigate users on the publicly available network.

In order to access Freenet, a user must first download the Freenet software, which is free and publicly available. (R. 23-1: Application, PageID 88). The Freenet "source code" — i.e., the computer programming code that facilitates Freenet's operation – is also publicly available. (Id.) Therefore, as TFO Anschutz restated - the open source Freenet software may be examined and analyzed by anyone with the pertinent expertise or knowledge.

TFO Anschutz further explained:

> Anyone running the Freenet software may join and access the Freenet network. Each computer running Freenet connects directly to other computers running Freenet, which are called its "peers." When installing Freenet, each user agrees to provide to the network a portion of the storage space on the user's computer hard drive, so that files uploaded by Freenet users can be distributed and stored across the network. Freenet users can upload files into the Freenet network and download files from the Freenet network. After a user installs Freenet on the user's computer, the software creates a default "download" folder. If a user successfully downloads a particular file from Freenet, Freenet may save the content of that file to the "download" folder. A user may change this default setting and direct the content to be downloaded elsewhere.
>
> When a user uploads a file into Freenet, the software breaks the file into pieces (called "blocks") and encrypts each piece. The encrypted pieces of the file are then distributed randomly and stored throughout the Freenet network of peers. The software also creates an index piece that contains a list of all of the pieces of the file and a unique key – a series of letters, numbers and special characters – that is used to download the file.
>
> In order to download a file on Freenet, a user must have the key for the file. There are a number of ways that a Freenet user can download a file using a key. Some examples include: (1) the "download" box on Freenet's "file sharing" page; (2) the "download" box on the message board associated with Freenet or other Freenet add-on programs; and (3) directly through the user's web browser while the user is connected to the Freenet network.
>
> When a user attempts to download a file via Freenet, Freenet downloads the piece of the file containing the index, which provides the information required to retrieve the individual pieces of the file. The Freenet software then requests all of the pieces of the file from the user's peers. *Rather than request all of the file pieces from a single peer, requests for file pieces are divided up in roughly equal amounts among the user's peers. If a user's peer does not have the particular requested pieces in its storage, that peer will then divide up and ask its peers for the pieces, and so on.* For example, if User "A" has 10 peers and requests 1000 pieces of a file, roughly 100 pieces are requested from each one of User A's peers. (Emphasis added) (Id. PageID 88-89).

The affidavit includes two diagrams that explain in a simple visual format how a user's request is divided among the first group of peers. If any or all of the first round of peers do not have the particular requested pieces, that peer will divide up again and ask its peers for the pieces. (Id. PageID 90). This aspect of the Freenet software makes it unique from other types of peer-2-peer programs. The affidavit further explains how the Freenet software is designed to prevent requests for pieces from going on indefinitely:

> Freenet is configured to only allow a request for a piece of a file to be forwarded to another peer a limited number of times (the default maximum is 18). The remaining number of times a request for a piece may be forwarded is included within the request for that piece. If a request reaches that limit without finding the requested piece, a signal is returned to the user's computer and the request is sent to another of the user's peers. (Id., PageID 91).

The affidavit then goes on to describe how the Freenet software attempts to hide which computer uploaded a file into or downloaded a file from the network. Freenet "mak[es] it difficult to differentiate whether a request for a piece that comes in from a peer originated with that peer (i.e., the peer was the "original requestor" of the file), or whether that peer was simply forwarding a different peer's request." (Id.). The affidavit continues:

> Freenet attempts to hide the identity of the original requestor by randomizing the initial number of times a request can be forwarded from one peer to another to be either 17 or 18. Without this randomization, any time a user received a request for a piece of a file that could be forwarded 18 times, the user would know that its peer was the original requestor of the file. This design allows investigators using Freenet to focus investigative efforts on peer computers that request pieces of files of interest that may be forwarded 17 or 18 times, in order to determine whether the peer was the original requestor of the file.
>
> Freenet has two operational modes, "Darknet" and "Opennet." On the Darknet mode, a computer connects only to peers whom the user has specifically selected. On the Opennet mode, a computer may connect to peers unknown to the user. A Freenet user may choose which mode to use. The mode relevant to this investigation involves a user who chose to use the Opennet operational mode.
>
> Freenet warns its users in multiple ways that it does not guarantee anonymity: when Freenet software is initially installed; within the log file each time Freenet is started; and via Freenet's publicly

> accessible website. Freenet software also does not mask a computer's IP address — the IP addresses of each Freenet user's peers are observable to the user. For example, if a user is connected to 10 peers on Freenet, all 10 of those peers' IP addresses will be observable to the user. The fact that Freenet does not mask IP addresses is explained on its publicly accessible website. Freenet also acknowledges on its publicly accessible website that, for users who use the Opennet mode, it can be statistically shown that a particular user more likely than not requested a file (as opposed to having merely forwarded the request of another peer) based on factors including the proportion of the pieces of a file requested by a user and the number of nearby peers. (Id. PageID 91-92).

The affidavit then further distinguishes Freenet from other peer-2-peer file sharing programs that allow a user to enter random search terms in search of child pornography files. According to the Affidavit:

> Unlike other file sharing systems, Freenet does not provide a search function for its users whereby users would insert search terms to locate files. Therefore, a user who wishes to locate and download child pornography from Freenet *must identify the key* associated with a particular child pornography file and then use that key to download the file. (Emphasis added)
>
> Freenet users can identify those keys in a number of ways. For example, "message boards" exist on Freenet that allow users to post textual messages and engage in online discussions involving the sexual exploitation of minors. Law enforcement agents have observed message boards labeled: "pthc," "boy porn," "hussy," "pedomom," "kidfetish," "toddler_cp," "hurtcore," and "tor-childporn." Typical posts to those message boards contain text, keys of child pornography files that can be downloaded through Freenet, and in some cases descriptions of the image or video file associated with those keys.
>
> Freenet users can also obtain keys of child pornography images or videos from websites that operate within Freenet called "Freesites." Freesites can only be accessed through Freenet. Some of those sites contain images of child pornography the user can view along with keys of child pornography files. It is also possible that Freenet users may obtain keys related to child pornography images or videos directly from other Freenet users.

Law enforcement and researchers at the University of Massachusetts Amherst studied the openly-available Freenet source code and analyzed activity on Freenet. (See Attachment A: Statistical Detection of Downloaders in Freenet). Seeing that users on Freenet distributed and downloaded child pornography, researchers created a statistical algorithm to determine the likelihood that a user was the original requestor of a piece of a file, in order to determine which users were requesting illicit child pornography files.

As in many other P2P law enforcement investigations, researchers created a law enforcement version of Freenet by modifying the openly-available source code. The law enforcement version of Freenet is used on the opennet operational mode of Freenet. It automatically logs certain information about requests it receives from its peers *in the normal operation of the Freenet system*. The information logged by the law enforcement version includes: the sender's IP address and Freenet location, "hops to live" value,[5] type of requests, the number of pieces of the file being requested, date and time of requests, the number of peers of the sender, and the requested keys (i.e., pieces of a file). All of this information is available to all users of Freenet. The law enforcement version of Freenet does not target specific computers and therefore the process by which Freenet selects peers for a user is unmodified.

The Affidavit describes the law enforcement version of the software. Most importantly, the Affidavit indicates that the law enforcement version of Freenet allows law enforcement to log information available to all standard Freenet users. The Affidavit specifically states:

> A modified version of the Freenet software is available to sworn law enforcement officers to assist in conducting Freenet investigations. I have been trained on the operation of the

[5] To prevent requests for pieces of files from being forwarded indefinitely, Freenet uses a "hops-to-live" counter. Generally, the value begins at 18 and is decreased by each relaying computer until it is zero, in which case a "notfound" error is returned.

> modified law enforcement version of Freenet. This law enforcement version is nearly identical to Freenet, except that it allows a computer operated by a law enforcement officer to automatically log information about requests for pieces of files received directly from its peers. The types of information logged by a law enforcement computer are available to all standard Freenet users as part of Freenet's normal operation. This information includes, but is not limited to: the IP addresses of the user's peers; the number of peers those peers report to have; a unique identifier assigned by the software (referred to as the computer's Freenet "location"); the remaining number of times a request for a piece of a file may be forwarded; the date/time of requests received from a peer; and the digital hash value of a requested piece.
>
> Law enforcement computers do not target specific peers on Freenet nor do law enforcement computers solicit requests from any peers. The Freenet information collected by law enforcement computers is logged and provided to other Freenet-trained law enforcement personnel in order to further investigations into Freenet users believed to be downloading child pornography files through Freenet.
>
> Law enforcement officers collect keys associated with suspected child pornography files that are being publicly shared and advertised on Freenet. Law enforcement only investigates Freenet users who request pieces of files associated with such keys collected by law enforcement. The keys collected by law enforcement have been obtained via publicly accessible sites, such as Freenet message boards and Freesites, as well as during the course of prior investigations into child pornography trafficking on Freenet. This investigation pertains to child pornography files with known keys, the content of which are further described below. Those files are referenced as "files of interest."
>
> By viewing the documented activity of a peer that sends a request to a law enforcement computer, it is possible to determine whether it is significantly more probable than not that the peer is the original requestor of a file of interest. Only those requests that were intended for law enforcement computers as recipients, that are forwarded 17 or 18 times, and are associated with a file of interest are analyzed. *A mathematical formula is then applied to determine the probability of whether the number of requests received for pieces of a file is significantly more than one would expect if the peer were merely forwarding the request of another computer*. (Emphasis added)

> Your affiant has reviewed a peer-reviewed, publicly-available academic paper describing the methodology of that mathematical formula. In basic terms, the methodology relies on two primary facts about the Freenet software: first, the original requestor divides up its requests for pieces of a file among its peers, sending a roughly equal fraction of the requests to each peer; second, if a peer does not have the requested pieces, the peer takes the fraction of requests for pieces of a particular file and divides them up again among its own peers. See Figures 1 and 2. Because a peer that is merely routing another peer's request would ask its peers for a significantly smaller portion of the pieces of a file than an original requester, it is possible for the recipient of requests to determine whether a request is significantly more likely than not from an original requestor. The academic paper's detailed evaluation finds that a formal mathematical formula based on this reasoning is highly accurate (specifically, it has a high true positive rate and a low false positive rate). Based upon my training and experience, I believe this to be a reliable method to determine whether it is significantly more probable than not that that a given Freenet computer is the original requestor of a file of interest.
>
> I am also aware through my training and experience that dozens of searches of digital devices have been conducted by law enforcement officers (either through court-authorization or consent) related to targets whose IP addresses were identified based upon analysis of information from Freenet law enforcement computers, pursuant to which evidence of child pornography possession and/or trafficking was located.

(Id. PageID 93-94).

III. ARGUMENT

A. POPA HAS FAILED TO PRODUCE EVIDENCE OF GOVERNMENT WRONGDOING AS IT RELATES TO THE LAW ENFORCEMENT SOFTWARE OR ESTABLISH MATERIALITY FOR HIS REQUEST TO PRODUCE THE LAW ENFORCEMENT VERSION OF FREENET

In short, the defendant contends that his "expert" requires a copy of this sensitive investigatory technology – which was used to log information about a request for pieces of known child pornography files from the defendant's IP address – for three reasons: to assess the reliability and functionality of the Freenet software; to assess pretrial motions; and to effectively cross-examine Agent Anschutz. (R. 23: Motion to Compel). This motion is based almost entirely on the affidavit of Tami Loehrs.

A careful review of the Loehrs affidavit supports the government's position that Popa has failed to meet his burden for the production of the modified law enforcement version of Freenet. First of all, the affidavit incorrectly asserts that Officer Anshutz did not provide in the search warrant affidavit "information regarding 'law enforcement tool', including whether that tool has been tested and validated, nor does he provide any log files created by the law enforcement tool as foundation for his opinions." (R. 23: Motion to Compel, PageID 74; R. 23-2: Affidavit of Loehrs, PageID 126). As noted above, the Affidavit provides extensive information regarding the law enforcement Freenet tool. (R. 23-1: Application, PageID 93-94). The Affidavit specifically mentions the peer-reviewed, publicly-available academic paper describing the methodology of the mathematical formula used by the law enforcement tool. (Id.) The government provided this academic paper to defense counsel on the same day she requested it. (See Attachment D: Email). Counsel complains that the government did not provide proof that the paper was published or peer reviewed, yet the paper itself contains a 2017 Copyright notation and reference to the IEEE International Workshop on Privacy Engineering in May of 2017 that reviewed the paper. In addition, the government provided supplemental discovery to counsel on February 19, 2019, that further documented the International Workshop on Privacy Engineering review process and the inclusion of the paper, in the organizations published materials. (See Attachments B and C).

Popa attached as an exhibit to his Motion to Suppress (R. 24) an article located on the freenetproject.org website titled Police Department's Tracking Efforts Based on False Statistics, dated May 26, 2016. (R. 24-3: Exhibit C, Freenet article). The article criticized the Missouri

Police Department's reliance on the "Hops to Live" number embedded in each request to determine if the request was from the originator. Popa incorrectly assumes the program used by TFO Anschutz used this same procedure and that this article is critical of the peer reviewed paper cited by TFO Anschutz in the Affidavit. It is not. First, a simple reading of the article compared to the description of the law enforcement Freenet program in the Affidavit makes it clear that TFO Anschutz was not relying solely on the Hops to Live number in the request. Second, the peer reviewed paper relied on by TFO Anschutz was vetted by the International Workshop on Privacy Engineering in May of 2017 and published in June of 2017. [See Attachment A: Statistical Detection of Downloaders in Freenet, Authored by Brian N. Levine, Marc Liberator, Brian Lynn, and Matthew Wright; Attachment B: Third International Workshop on Privacy Engineering, Table of Contents; an Attachment C: Preface on the International Workshop on Privacy Engineering 2017, May 2017). A full year after the article attached by the defendant.

Second, the government provided the Freenet log files to Popa one week after he requested them for the first time in the Motion to Compel. (See Attachment E: Email regarding supplemental discovery). If this material was critical to Ms. Loehrs evaluation of the Freenet evidence, then it should have been requested and reviewed before Ms. Loehrs opined that it was necessary to conduct an independent analysis of the veracity of the law enforcement tool. In fact, it appears that Ms. Loehrs is not familiar with the Freenet program and/or did not review the Freenet website to understand the volume of information that is publicly available when a request is made by a user in the opennet operational mode of Freenet.

There are a number of statements in the Loehrs affidavit that would suggest this. For example, in ¶15 Ms. Loehrs discusses hidden dangers of file sharing software including the download of unwanted material. This statement seems to be a stock assertion in other peer-2-

peer investigations where law enforcement downloads suspected images of child pornography from a suspect's computer that is making images available. The claim is that a user on a typical peer-2-peer program could download an image or video only to learn that it was not what they wanted so they immediately delete it. However, Freenet is a completely different type of peer-2-peer program. Law enforcement is not downloading child pornography from the user's shared file after entering common child pornography search terms to find people sharing the material. They are looking for users that are requesting pieces of a known child pornography file using specific and lengthy alpha numeric keys.

As noted above, a Freenet user does not search by random search terms for files. In order to download a file on Freenet, a user must have the key for the file. There are a number of ways that a Freenet user can download a file using a key. Some examples include: (1) the "download" box on Freenet's "file sharing" page; (2) the "download" box on the message board associated with Freenet or other Freenet add-on programs; and (3) directly through the user's web browser while the user is connected to the Freenet network. When a user attempts to download a file via Freenet, Freenet downloads the piece of the file containing the index, which provides the information required to retrieve the individual pieces of the file. (R. 23-1: Application, PageID 88-89).

Moreover, the discovery in this case did in fact establish that the pieces of the horrific video (depicting the use of an ice cube to torture an infant) requested by Popa on April 21, 2018, between 9:30 am UTC and 10:04 am UTC, were acknowledged by Popa in his interview and found on his laptop computer during a forensic analysis. (R. 1: Criminal Complaint, ¶¶13-14, filed under seal).

Second, the Loehrs affidavit complains that "Officer Anschutz avers in his affidavit that the IP address associated with Mr. Popa *contains* child pornography based on incomplete files reported by his law enforcement tool and then describes completed files that he downloaded from other sources." Again, this shows a complete lack of understanding of the Freenet program on her part. The Affidavit does not allege that Popa's IP address *contains* child pornography. It clearly states that the IP address later associated with Popa was *requesting*, using very specific alpha numeric keys, approximately 1/13th of a known child pornography file. To verify that this file and these keys were still available on Freenet, TFO Anschutz downloaded the entire file to confirm it was, in fact, a video containing child pornography. (Emphasis added)

To further confuse matters, Ms. Loehrs states the following:

> According to the affidavit of Officer Anschutz, this case originated in April, 2018 when "a computer running Freenet software, with an IP address of 173.90.126.69, with 13.1 peers, requested from a law enforcement computer 136 out of 1786 total pieces needed to assemble a file with a SHA1 digital hash value of ATLOOVASIDQV6JPN***************." That is, the computer at the suspect IP address reportedly requested less than .075% of a file which would likely render that file non-viewable and would not, in that incomplete state, contain child pornography. Officer Anschutz then downloaded the completed file from someone other than the suspect and describes the content of the completed file in his Affidavit. This activity occurred for several additional files, none of which the suspect reported having 100% of the content. (redacted)

(R. 23-2: Affidavit of Loehrs, PageID 123). This is just further evidence of Ms. Loehrs lack of knowledge about the Freenet software, at best, or an intentional effort on her part to mislead the Court. As described in the Affidavit, the Freenet software divides up the request of the original requester equally among his/her peers. During that download, Popa had an average of 13.1 peers, so the first request would have been divided up into approximately 13 different requests for pieces. If the file had 1,786 total pieces, 1/13th of that file would be approximately 137 pieces. According to the Affidavit, the request was for 136 pieces. Therefore, based upon the way the Freenet software divides up a request for a whole file by asking for pieces from peers, in this case 13, this fact helped to establish probable cause to believe that this was the original requestor asking for the entire child pornography file fully downloaded by TFO Anschutz. To put it another way, if Popa only intended to collect a small part of a larger child pornography file like 136 pieces (the non-child pornography pieces of course), that request would have been broken up by the software into only about 10 pieces per peer.

As a final example, Ms. Loehrs affidavit states she has experience on Freenet cases and her Curriculum Vitae lists numerous federal child exploitation cases where she has testified for the defense. Despite the way in which she repeatedly trashes law enforcement tools, Ms. Loehrs does not list even one case where she was permitted to examine/validate the law enforcement modified version of a publicly-available peer-2-peer program and she discovered that it incorrectly collected data or accessed information on a user's computer that was not otherwise publicly available.

B. THE DEFENDANT HAS FAILED TO MEET HIS THRESHOLD BURDON OF MATERIALITY

Popa fails to establish why a copy of the law enforcement sensitive program, above and beyond the discovery already provided, is material to the preparation of his defense. Federal Rule of Criminal Procedure 16 requires the government to disclose, upon the defendant's request, all "documents . . . within the government's possession, custody, or control . . . [that are] material to preparing the defense." Fed. R. Crim. P. 16(a)(1)(E)(i). In order to compel disclosure, "a defendant must make a threshold showing of materiality." United States v. Santiago, 46 F.3d 885, 894 (9th Cir. 1995); see also United States v. Ross, 511 F.2d 757, 762 (5th Cir. 1975) (defendant must demonstrate that the sought-after information bears more than some "abstract logical relationship to the issues in the case"). It is the defendant's burden to proffer what potential defense could be supported by what specific type of information is purportedly contained in the requested materials, and "[n]either a general description of the information sought nor conclusory allegations of materiality suffice; a defense must present facts which would tend to show that the Government is in possession of information helpful to the defense." United States v. Mandel, 914 F.2d 1215, 1219 (9th Cir. 1990); see also United States v. Pirosko, 787 F.3d 358, 367-68 (6th Cir. 2015); and United States v. Carrasquillo-Plaza, 873 F.2d 10, 12-13 (1st Cir. 1989).

Here, the defense "expert," Tami Loehrs, presents exactly what the courts have proscribed: a general description of the information sought, and conclusory allegations of materiality. According to Ms. Loehrs, she did not review log files in this case before preparing her affidavit. Further, Ms. Loehrs admits that she did not perform an independent review of Popa's computer evidence. She opines that her experience on "hundreds of cases throughout the country involving law enforcement's investigations of P2P and BitTorrent file sharing networks, including the use of Freenet," has "brought to light serious issues with regard to the accuracy and reliability of the proprietary software used by law enforcement." (R. 23-2: Loehrs Affidavit, PageID 123). Yet she fails to name one case to support this statement. Nevertheless, she extrapolates that an examination of the law enforcement tool is necessary to determine its reliability and accuracy. This allegation is eerily similar to allegations made by Ms. Loehrs in other cases involving other law enforcement software using wholly different P2P networks and protocols.

Ms. Loehrs did not examine the evidence in this case and makes numerous inaccurate or misleading statements in her affidavit. Other than her vague assertions casting doubt upon the validity of these law enforcement tools based on her "past experience" – with no concrete facts or examples – she has not offered any concrete basis to meet the threshold burden of establishing materiality. As a federal district judge in the District of Massachusetts aptly put it: "[t]he defendant has not made a prima facie showing of materiality. . . . He essentially seeks access to the government's information haystack because he is confident there are useful evidentiary needles to be found there. That is simply not enough to trigger a disclosure obligation under Rule 16(a)(1)(E)(i)." United States v. Tsarnaev, 2013 WL 6196279, at *5 (D. Mass. 2013); see also United States v. Chiaradio, 684 F.3d 265 (1st Cir. 2012) (finding that peer review was not required in order for law enforcement to use a similar P2P program).

Providing "expert" support for speculative discovery requests is nothing new for the defendant's supposed expert. In fact, Ms. Loehrs has made similar assertions in prior cases – several of which met withering criticism from the presiding judges. In United States v.Thomas, Neale, and Leikert, 2013 WL 6000484 (D. Vt. 2013), a group of defendants filed a series of motions, including a similar motion to compel the production of another law enforcement P2P investigative program. In support of the motion, Ms. Loehrs raised equally vague concerns about the absence of any prior third party validation of the P2P law enforcement tool. Chief Judge Reiss of the United States District Court for the District of Vermont was not impressed with the quality of Ms. Loehrs' work, finding:

> Ms. Loehrs's declarations filed in Neale and Leikert are misleading in several respects. For example, in each of them, Ms. Loehrs stated that she needed to test Peer Spectre software [the law enforcement tool] because 'this is the very same automated software used by law enforcement in numerous cases throughout the country in which I have been involved as a defense expert. These cases have brought to light serious concerns with regard to the . . . software used by law enforcement during undercover P2P investigations[.]' She further testified that peer-to-peer software is not validated, tested, or reliable, noting specifically that 'Peer Spectre in any searching does rely on the reliability of these networks that we're searching. And these networks are horribly unreliable.' She conceded that there is no available protocol for testing peer-to-peer file

> sharing software. She cites no court and no learned treatise or peer-reviewed research that has endorsed her concerns. She also cited no evidence that any court has granted a motion to suppress based on her testimony or has expressed 'serious concerns' with law enforcement's use of Peer Spectre or with any other CPS products.
> As a preface to a list of twenty-five cases identified in her declarations, Ms. Loehrs stated: 'I have also learned through hundreds of forensic examinations on cases involving undercover P2P investigations and allegations of child pornography, that files are being identified by law enforcement's automated software as containing child pornography when, in fact, they do not. However, none of the cases listed in Ms. Loehrs's declarations appeared to have resulted in judicial findings to that effect.
> [. . . .]
> [I]n her declaration Ms. Loehrs noted that the specific images identified in the Leikert search warrant application were not later found on [the defendant's] computer. She again notes that the government's forensic report reflects the same finding. On cross-examination, however, she acknowledged that [the defendant] re-installed the operating system of his computer before the search warrant's execution. In such event, she acknowledges that any pre-existing files would be destroyed. Again, this fact was not disclosed in her declaration.

(Id.).

The court later found that one of Ms. Loehrs's claims was "either incredible or reflective of a lack of concern regarding the reliability of the opinions she is offering under oath." The Court ultimately concluded that, "on balance, Ms. Loehrs provided little, if any, credible or reliable testimony to support her expert opinions in this case," and therefore did "not rely on her opinions in reaching its conclusions." Opinion and Order Denying Defendants' Motion to Suppress, United States v. Thomas, Neale, and Leikert, 2013 WL 6000484, *15-16 (D. Vt. Nov. 8, 2013).

Loehrs' credibility was also questioned in State of Arizona v. Robert Dean Moran, in which she made comparable claims about the need to analyze another law enforcement P2P investigative tool. CR2009-114677-001 SE (Maricopa County Superior Court Sept. 11, 2012). After Loehrs expressed opinions similar to those contained in her affidavit here, the Moran court squarely rejected those opinions, finding that "Ms. Loehrs . . . could not explain her own testing methods based on her screenshots she provided," and that, "[o]verall, [Ms. Loehrs] provided testing screen captures to this Court that were inaccurate, incomplete, and thus misleading as they did not fully set forth in detail the testing she asserts . . . supports her contention that there are flaws with the Peer Spectre program." Id.

More recently, the Court of Appeals for the Sixth Circuit reflected on Loehrs's credibility, noting, before rejecting the defendant's motion to compel production of a law enforcement investigative tool, that the district court in Thomas had "considered and completely discredited Loehrs' statements." See United States v. Pirosko, 787 F.3d 358, 367 (6th Cir. 2015); see also United States v. Mitchell, 128 F.Supp.3d 1266, 1268-69 (E.D. Ca. 2015) (describing how Tami Loehrs "acknowledged that several of the statements included in her first declaration were incorrect because she conducts many exams at off-site locations and she had confused her site visit in this case with a separate visit to San Francisco for a different case"). Many of those same problems – including speculative assertions, and lack of legal and forensic support for those assertions – are also prevalent here.

Nevertheless, regardless of the defense expert's credibility or lack thereof, several courts, including the Court of Appeals for the Sixth Circuit, have denied similar motions to compel the production of a law enforcement P2P investigative tool or its source code. See, e.g., United States v. Pirosko, 787 F.3d 358, 366-67 (6th Cir. 2015) (affirming district court's denial of defendant's motion to compel production of law enforcement investigative tool, in part because the defendant did not "produce . . . evidence of government wrongdoing", and reasoning that "allowing [the defendant] access without any evidence of error would needlessly expose the government's enforcement tools to examination and pointlessly drag out the course of litigation"); United States v. Chiaradio, 684 F.3d 265, 277-78 (1st Cir. 2012) (affirming denial of defense request for underlying source code of law enforcement child pornography P2P investigative tool, in part highlighting the fact that the source code (and thus, the program), was purposely kept secret because the government "reasonably fears that traders of child pornography (a notoriously computer-literate group) otherwise would be able to use the source code to develop ways either to evade apprehension or to mislead the authorities," which satisfactorily explained the absence of any peer review); United States v. Feldman, 2015 WL 248006, at *6 (E.D. Wis. 2015) (denying defendant's motion to compel production of law enforcement P2P investigative tool because defendant failed to establish materiality); United States v. Brashear, 2013 WL 6065326 (M.D. Pa. Nov. 18, 2013) (holding that source code was not discoverable); State v. Roberts, 2015 WL 404627 (Utah S.Ct. 2015) (trial court did not abuse its discretion in denying defendant's motion to compel discovery of law enforcement P2P software); State v. Wilkie, 88 N.E. 3d 1196 (Ohio App. 2017) (holding that the trial court properly denied defendant's motion to obtain copy of law enforcement P2P program and accompanying documents); cf. United States v. Boxley, 373 F.3d 759, 761 (6th Cir. 2004) (stating that, with respect to dog sniffs, "it is not necessary for the government to show that the dog is accurate one hundred percent of the time, because a very low percentage of false positives is not necessarily fatal to a finding that a drug detection dog is properly trained and certified"); United States v. Dillow, 2013 WL 5863024 (N.D. Oh. 2013) (that local law enforcement had computer software used to establish defendant's possession of child pornography did not mean that federal prosecuting attorneys had possession of the software, or that they were obligated to obtain it, such that the defendant was not entitled under the rule governing discovery in criminal proceedings to inspect the software).

The defendant – as defendants often do, in cases involving Ms. Loehrs' quest for proprietary law enforcement source code – relies predominantly on United States v. Budziak, 697 F.3d 1105 (9th Cir. 2012), to support his request for discovery. The facts in Budziak, however, are easily distinguishable. There, the defendant was charged, among other things, with distribution of child pornography. The government's evidence included, inter alia, child pornography files downloaded remotely from the defendant's computer through the use of a P2P investigative tool. The defendant stipulated to all elements of the offense except for knowing distribution, making the P2P-derived evidence atypically central to the government's burden of proof at trial. The defendant also presented specific evidence suggesting that the investigating officer may have only downloaded fragments of child pornography from the defendant's "incomplete" folder, thus making it "more likely" that he did not knowingly distribute any complete child pornography files to agents; and submitted specific evidence suggesting that the investigators could have used the software to override his "sharing" settings. In contrast to the First Circuit in Chiaradio, the Ninth Circuit held that the government should therefore have disclosed a law enforcement P2P tool to the defendant, in order for his expert to answer those specifically articulated questions that were supported by actual forensic evidence.

Budziak is a far cry from the facts presented in the instant matter. Unlike in Budziak, the defense in this case has neither identified any specific evidence of government error or improper intrusion, nor articulated any particular need for unfettered access to the law enforcement modified version of Freenet, and has thus failed to meet its burden of demonstrating materiality.

C. SENSITIVE LAW ENFORCEMENT SURVEILLANCE SOFTWARE IS PROTECTED BY QUALIFIED PRIVILEGE AND SHOULD NOT BE PRODUCED IN DISCOVERY

Courts throughout the country have recognized the existence of a law enforcement privilege, and have used that privilege as a basis to deny discovery requests such as this one. See, e.g., United States v. Cintolo, 818 F.3d 980, 1002-1003 (1st Cir. 1987) (recognizing "the policy of qualified privilege to be entirely appropriate . . . where a defendant seeks disclosure of confidential government surveillance information"); In re Department of Investigation of the City of New York v. Myerson, 856 F.2d 481, 484 (2d Cir. 1988); United States v. Van Horn, 789 F.2d 1492, 1507 (11th Cir. 1986) (recognizing "a qualified governmental privilege not to disclose sensitive investigative techniques" which therefore protected disclosure of the type and location of microphone used in undercover recordings). The purpose of the privilege is "to prevent disclosure of law enforcement techniques and procedures, to preserve the confidentiality of sources, to protect witness and law enforcement personnel, to safeguard the privacy of individuals involved in an investigation, and otherwise to prevent interference with an investigation." In re Dep't of Investigation, 856 F.2d at 484; Commonwealth of Puerto Rico v. United States, 490 F.3d 50, 64 (1st Cir. 2007).

The government bears the initial burden of showing that the law enforcement privilege applies to the materials at issue, In re The City of New York, 607 F.3d 923, 944 (2d Cir. 2010), and the court must then apply a balancing test in determining whether disclosure is required, Van Horn, 789 F.2d at 1508. The court should consider the defendant's "need [for] the evidence to conduct his defense and [whether] there are . . . adequate alternative means of getting at the same point. The degree of the handicap [to the defendant] must then be weighed by the trial judge against the policies underlying the privilege." Harley, 682 F.2d at 1020; Cintolo, 818 F.2d at 1002.

The First Circuit, in United States v. Chiaradio, 684 F.3d 265, 278 (1st Cir. 2012), recently considered whether this qualified privilege applied to the source code for EP2P, a law enforcement version of a peer-2-peer program. While the court in Chiaradio did not ultimately base its denial of the defendant's motion to compel on the law enforcement privilege, the court strongly implied that the privilege would operate to bar discovery in such a case "because the government reasonably fears that traders of child pornography (a notoriously computer-literate group) otherwise would be able to use the source code to develop ways either to evade apprehension or to mislead the authorities." Chiaradio, 684 F.3d at 278. This is precisely the concern at issue here.

The law enforcement modified version of Freenet, created exclusively for use in law enforcement investigations, is a sensitive law enforcement technique. Although the software has been distributed for use to federal, state and local law enforcement agencies, the developers have taken steps to protect and maintain the sensitive nature of the software: first, only licensed law enforcement officers can use the program, and they do not have permission to disclose copies of the program; and second, the source code of the program is locked to prevent examination of the software by anyone, including the law enforcement agents using the software to conduct investigations. Therefore, release of the software may jeopardize many ongoing investigations and potentially destroy the integrity of the Program in hundreds of cases around the country. See United States v. Harley, 682 F.2d 1018 (D.C. Cir. 1982) (discovery of listening post not required to support identification of defendant where disclosure would jeopardize safety even when post no longer used).

Providing the defense with access to Freenet law enforcement program would also expose the full universe of child pornography images (designated by hash values and keys) previously identified by law enforcement agents using the tool. This would have the same impact, essentially, as disclosing a hidden observation post: if offenders knew which child pornography files law enforcement was searching for, they could simply trade other files, or alter a single pixel in files contained in the law enforcement database so that those files generated an entirely different hash value, thus completely frustrating the efforts of investigators. Cf., e.g., Van Horn, 789 F.2d at 1507 ("[T]he identification of a hidden observation post will likely destroy the future value of that location for police surveillance."). Disclosure of the hash value database is also problematic for a second reason: it would provide offenders with a road map for how to more efficiently obtain the listed child pornography files, because each hash value specifically identifies a particular child pornography file shared on P2P networks. If even a single offender was able to obtain this database, there is no doubt that it would become an immensely valuable commodity for the greater offender community, and be rapidly shared among that group. After all, nothing would be more valuable to those who seek out child pornography than a list enabling the easy acquisition of thousands of the worst child pornography images and videos. This is a particular worry as to Ms. Loehrs, who previously inadvertently attempted to remove contraband child pornography images from a government facility. See United States v. Arter, 07-CR-020-GEB (E.D. Calif. 2007), Document 37.

Disclosing sensitive details about these investigative tools could also permit other offenders to more easily identify undercover law enforcement agents and thus evade detection. For example, because there are so many client software programs for each network, if offenders are aware of which version of the software law enforcement employs, they could potentially avoid sharing child pornography files with users employing that particular version, thereby thwarting law enforcement's undercover operations across the board.

D. DEFENDANT'S IP ADDRESS WAS PROPERLY OBTAINED BY AN ADMINISTRATIVE SUBPOENA.

In his first argument, Defendant alleges that obtaining his IP address through an administrative subpoena violated Carpenter v. United States, 138 S. Ct. 2206, 201 L.Ed2d 507 (2018). Defendant provides merely a conclusory statement that "the administrative subpoena issued in the instant case for the information stored at Time Warner is akin to the information at issue in Carpenter and, therefore, the Government obtained it in violation of Mr. Popa's Fourth Amendment right." (R. 24: Def's Motion, PageID 158). He provides no authority in support of this argument, other than dicta. Neither Carpenter nor Jones overturned the requirements to obtain basic subscriber information pursuant to 18 U.S.C. § 2703(c), in fact neither case even dealt with that statute.[6]

The government's acquisition of defendant's IP address is governed by 18 U.S.C. § 2703(c)(2) which states:

> (c) Records concerning electronic communication service or remote computing service.--(1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity--
>
> (A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures and, in the case of a court-martial or other proceeding under chapter 47 of title 10 (the Uniform Code of Military Justice), issued under section 846 of that title, in accordance with regulations prescribed by the President) by a court of competent jurisdiction;
>
> (B) obtains a court order for such disclosure under subsection (d) of this section;
>
> (C) has the consent of the subscriber or customer to such disclosure;
>
> (D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such

[6] Both Carpenter and United States v. Jones, 565 U.S. 400 (2012), involved orders obtained under 18 U.S.C. § 2703(d). Jones held that evidence obtained pursuant to § 2703(d), by the warrantless use of a GPS device violated the Fourth Amendment. Carpenter held that evidence obtained pursuant to § 2703(d), by the warrantless use of a cell-site location data violated the Fourth Amendment.

> provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or
>
> (E) *seeks information under paragraph* (2).
>
> *(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the--*
>
> *(A) name;*
>
> *(B) address;*
>
> *(C) local and long distance telephone connection records, or records of session times and durations;*
>
> *(D) length of service (including start date) and types of service utilized;*
>
> *(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and*
>
> *(F) means and source of payment for such service (including any credit card or bank account number),*
>
> *of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1). (Emphasis added).*
>
> (3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.

A search warrant is not required to obtain basic subscriber information from a private entity, such as Time Warner Cable, when law enforcement obtains a grand jury subpoena and limits the request to basic information such name, address, associated phone numbers, length of service, IP address, and source of payment.[7] In the present case, FBI TFO Anschutz properly

[7] Basic subscriber information is not "content" of communications. See United States v. Graham, 824 F.3d 412, 433 (4th Cir. 2016).

obtained an administrative subpoena under § 2703(c)(2) to Time Warner Cable for the production of non-content basic subscriber information to determine defendant's IP address.

Defendant's undeveloped argument that Carpenter is authority that basic subscriber information must be obtained with a search warrant is unsupported and misguided. Carpenter involved the use of cell site location data which was previously authorized under 18 U.S.C. § 2703(d). Unlike § 2703(c)(2), § 2703(d) specifically required a court order based upon specific and articulable facts showing reasonable grounds to believe the contents of a wire or electronic communication were relevant and material to an ongoing criminal investigation. Carpenter held that "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured by CSLI [cell site location]," and therefore, a court order under § 2703(d) is insufficient, and a search warrant is required. Id. at 2217.

Defendant fails to draw any correlation between basic subscriber information and a record of his physical movements by GPS or cell site location, nor does he explain his expectation of privacy in basic subscriber information. He further fails to explain the contradiction of his argument with the authorizing statute, which clearly states an administrative subpoena may be issued for basic subscriber information. Basic subscriber information obtained by law enforcement would not allow them to track his physical movements as in Jones and Carpenter, nor was § 2703(c)(2) the subject of either case. In fact, § 2703(c)(2) does not implicate the "third-party" doctrine relied upon by the defendant.

Defendant asks this Court to wildly leap from the requirements of § 2703(c)(2), go past a § 2703(d) "reasonable grounds" showing to obtain a court order, and land squarely on a search warrant requirement. Even Carpenter recognized that its holding was limited to a specific category of cases. "This is certainly not to say that all orders compelling the production of documents will require a showing of probable cause. The Government will be able to use subpoenas to acquire records in the overwhelming majority of investigations. We hold only that a warrant is required in the rare case where the suspect has a legitimate privacy interest in records held by a third party." Carpenter at 2222. Defendant's argument that his basic subscriber information must be obtained by a search warrant is unsupported by statute or case law, and should be denied.

E. THE RESIDENTIAL SEARCH WARRANT WAS AMPLY SUPPORTED BY PROBABLE CAUSE AND LAW ENFORCEMENT REASONABLY RELIED IN GOOD FAITH UPON ITS AUTHORIZATION

1. The Residential Search Warrant was Amply Supported by Probably Cause

The Fourth Amendment provides that "no warrant shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV; See United States v. Murphy, 241 F.3d 447 (6th Cir. 2001). "[P]robable cause is a flexible, common-sense standard. It merely requires that the facts available to the officer would 'warrant a man of reasonable caution in the belief' that certain items may be contraband or stolen property or useful as evidence of a crime; it does not demand any showing that such a belief be correct or more likely true than false." Texas v. Brown, 460 U.S. 730, 742 (1982).

The task of the issuing magistrate is simply to make a practical, common sense decision whether, given all of the circumstances set forth in the affidavit before him, including the 'veracity' and 'basis of knowledge' of persons supplying hearsay information, there is a fair probability that contraband or evidence of a crime will be found in a particular place. Only the probability, and not a prima facie showing, of criminal activity is the standard of probable cause. And the duty of a reviewing court is simply to insure that the magistrate had a substantial basis for concluding that probable cause existed. Illinois v. Gates, 462 U.S. at 230. A probable cause determination will be upheld if the issuing judge or magistrate had a substantial basis for concluding that a search would uncover evidence of wrongdoing. Id. A reviewing court must give great deference to a magistrate's determination of probable cause for issuance of a search warrant, and may reverse a magistrate's decision to grant a search warrant only if the magistrate arbitrarily exercised his or her authority. U.S. v. Brown, 732 F.3d 569 (6th Cir. 2013).

The affidavit in support of the search warrant in this case provided ample information for Magistrate Judge Limbert to conclude that there was a fair probability that evidence of child pornography would be located on digital devices in Popa's home. Indeed, the affiant's assessment—and the magistrate's reasonable reliance upon it—was supported by specific, articulable facts and inferences drawn from TFO Anschutz's training and experience. For example, the affidavit first sought to inform the magistrate about essential and technical information underlying the investigation. TFO Anschutz set forth a thorough explanation of what Freenet is, how it operates, and the use of the modified version of Freenet by law enforcement to analyze user requests. A full-page "definitions" section describing a number of technical terms and concepts related to Freenet and the investigation was included to assist the magistrate. The affidavit explained that Freenet is a distributed, Internet based, P2P network which attempts to let a user anonymously share files and chat on forums. Further, that communications between computers running Freenet are routed through other computers running Freenet, which makes it difficult to determine who is the original requestor of information. TFO Anschutz explained to the magistrate that files are stored on Freenet using a key and that Freenet breaks files into pieces, distributes the pieces across the network and stores them on disk space provided by Freenet users. It was also explained to the magistrate how a user downloads a file on Freenet. For instance, the affidavit stated that a user inserts a key to a file and once inserted, requests are sent to a user's peers for pieces of the file and if a peer does not have the piece, the request is relayed to the peer's peer.

TFO Anschutz outlined for the magistrate how the investigation into Freenet began in September 2011. He explained that law enforcement started collecting keys on Freenet associated with child pornography. Also, that law enforcement started running a modified version of Freenet and logged information about requests received. Importantly, the affidavit explained that streams of requests for pieces of files from particular IP addresses can be evaluated to determine whether the user of an IP address is the likely original requestor of a file by analyzing data and certain characteristics associated with the request and inputting such information into a mathematical formula.

After providing such essential background on Freenet and the investigation into Freenet, the affidavit tailored probable cause information related to this case by describing three files that were requested by the user of IP address 173.90.126.69, which files TFO Anschutz independently downloaded and verified to have contained child pornography. The affidavit included the date and times of the requests, the IP address associated with the requests, the file names, and the digital hash value of the files, along with a description of their content. Most significantly, the affidavit explained that the number and timing of the requests for particular child pornography files received by the law enforcement computer was significant enough to indicate that IP address 173.90.126.69 was the apparent original requestor of the three files.

The affidavit then articulated the further investigative steps that led law enforcement to Popa's home – explaining that IP address 173.90.126.69 was registered to Time Warner Cable and that Time Warner records indicated that IP address was registered to "James Skelly," at the at 533 Redwood Street SW, email address wowsaddie@twc.com, telephone number 330-324-XXXX, account number 20638XXXX and the active IP address date of 12/19/2017. (redacted)

TFO Anschutz laid out information regarding his background as an investigator. He detailed his training relevant to his assignment in the Child Exploitation Task Force, to include his training on Freenet investigations. The affidavit further explained how computers and other digital devices work and are used to store child pornography. Finally, the affidavit and attachments described with particularity Popa's residence (the place to be searched) and the items to be seized.

Popa focuses his entire attack of the search warrant affidavit on the reliability of the law enforcement program and the mathematical formula it relies up. In United States v. Schumacher, Case No. 14-3576, Doc. 31-1: Opinion (6th Cir. 2015) (unreported), the Sixth Circuit rejected an argument identical to the one advanced by Popa herein. Schumacher argued that the veracity of the entire search warrant affidavit was in doubt because the affidavit "provide[d] no information relative to the accuracy or reliability of the government's method of investigation," and that the affidavit did not describe how the investigative software worked, or cite statistics or a single report verifying its claims as to reliability and accuracy. (Id. at p. 4). The Court concluded that the inclusion in the affidavit of a more detailed account of how the software operated, and statistics and reports verifying its reliability and accuracy would have arguably only strengthened, not decreased, the affidavit by showing that the software was reliable and that a search would turn up images of child pornography. (Id. at pp. 4-5, citing United States v. Chiaradio, 684 F.3d 265, 279 (1st Cir. 2012)).

2. Even if the Affidavit Was Not Supported by Probable Cause, the Good Faith Exception in United States v. Leon Applies

Ordinarily, when a search violates the Fourth Amendment, the fruits thereof are inadmissible under the exclusionary rule, "a judicially created remedy designed to safeguard Fourth Amendment rights generally through its deterrent effect." See United States v. Calandra, 414 U.S. 338, 348 (1974). The exclusionary rule's sole purpose is to deter future Fourth Amendment violations, e.g., Herring v. United States, 555 U.S. 135, 141 (2009), and its operation is limited to situations in which this purpose is "thought most efficaciously served," Calandra, at 348. For exclusion to be appropriate, the deterrence benefits of suppression must outweigh the rule's heavy costs. As such, in Leon, the Supreme Court established a good faith exception to the exclusionary rule under which "evidence obtained pursuant to a search warrant issued by a neutral magistrate does not need to be excluded if the officer's reliance on the warrant was objectively reasonable." Id. at 461. Usually, "'a warrant issued by a magistrate ... suffices to establish' that a law enforcement officer has 'acted in good faith in conducting the search.'" Leon, 468 U.S. at 922 (quoting United States v. Ross, 456 U.S. 798, 823 (1982). Accordingly, searches executed "'pursuant to a warrant will rarely require any deep inquiry into reasonableness.'" Id. (quoting Gates, 462 U.S. at 267).

The Leon rule validates a search based on an invalid warrant unless: (1) the supporting affidavit contained knowing or reckless falsity; (2) the issuing judge wholly abandoned his judicial role; (3) the affidavit is so lacking in probable cause as to render official belief in its existence entirely unreasonable; or (4) the officer's reliance on the warrant was neither in good faith nor objectively reasonable. United States v. Abboud, 438 F.3d 554, 578 (6th Cir. 2006).

In this case, none of the four Leon factors are present and thus if probable cause did not exist, law enforcement's reliance on the warrant was objectively reasonable. As outlined in

Sections and F below, there are no false statements or material omissions in the affidavit to trigger the first Leon exception. Further, there is no evidence to suggest that Magistrate Limbert abandoned his judicial role. Third, after reviewing the request for specific keys/pieces that make up a known child pornography file, applying the mathematical formula vetted by a peer-reviewed paper, and verifying that the entire file was in fact available on Freenet and constituted child pornography, it was reasonable for TFO Anschutz to conclude there was probable cause to believe he would find evidence of child pornography on a device at the target residence. And finally, the warrant detailed the investigation, the particular place to be searched and the evidence to be seized. TFO Anschutz had no reason to believe the warrant was facially deficient, or that he should not objectively rely upon it. Therefore, even if it is determined probable cause did not exist, the good faith exception set forth in Leon applies and the evidence should not be suppressed.

F. POPA HAS FAILED TO MAKE A SUBSTANTIAL PRELIMINARY SHOWING OF A FALSE CLAIM IN THE SEARCH WARRANT AFFIDAVIT

Popa's sole allegation in support of his request for a hearing pursuant to Franks v. Delaware (1978), 438 U.S. 154, is that TFO Anshutz's statement regarding a peer-reviewed article "does not appear to be true." (R. 24: Motion to Suppress, PageID159-160). The government extensively discusses above the peer-reviewed literature relied upon by TFO Anschutz in the Affidavit to search Popa's residence and computer devices. The portion of the article attached to Popa's motion attacking police department's tracking efforts predated the government's peer-reviewed literature by one year. The protocol outlined in that letter is not the same protocol outlined in the Affidavit.

A defendant may challenge the legality of a search warrant affidavit if he can preliminarily establish a false statement, necessary to the finding of probable cause, is contained within the affidavit. Franks v. Delaware, 438 U.S. 154, 155. (1978). A defendant is entitled to a Franks hearing if he (1) "makes a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit," and (2) "the allegedly false statement is necessary to the finding of probable cause." United States v. Graham, 275 F.3d 490, 505 (6th Cir.2001) (internal quotation marks omitted). We have previously explained that "[a] defendant who challenges the veracity of statements made in an affidavit that formed the basis for a warrant has a heavy burden." United States v. Bennett, 905 F.2d 931, 934 (6th Cir.1990).

> A defendant who challenges the veracity of statements made in an affidavit that formed the basis for a warrant has a heavy burden. His allegations must be more than conclusory. He must point to specific false statements that he claims were made intentionally or with reckless disregard for the truth. He must accompany his allegations with an offer of proof. Moreover, he also should provide supporting affidavits or explain their absence. If he meets these requirements, then the question becomes whether, absent the challenged statements, there remains sufficient content in the affidavit to support a finding of probable cause.
>
> If probable cause exists absent the challenged statements, a defendant is entitled to no more; however, if such cause does not exist absent the challenged statements, he is entitled to a hearing if he requests one. He must show at the hearing, by a preponderance of the evidence, that false statements were made either intentionally or with reckless disregard for the truth and that without these statements there is insufficient content in the affidavit to support a finding of probable cause. If he makes this showing, the evidence should be suppressed.

905 F.2d at 934.

The first prong of the Franks analysis (whether the defendant has made a substantial preliminary showing of intentional or reckless falsity) is a factual question that we evaluate under the clear-error standard. See United States v. Poulsen, 655 F.3d 492, 504 (6th Cir.2011) ("The determination as to whether a statement made in an affidavit is made with reckless disregard of the truth is a fact question.") (internal quotation marks omitted); see also Graham, 275 F.3d at 505 ("[T]he district court's factual findings are reviewed for clear error."). If a defendant makes this substantial preliminary showing, we turn to the second prong of the Franks analysis by removing the allegedly false statement and asking whether the search-warrant affidavit still supports a finding of probable cause. Graham, 275 F.3d at 505.

The second prong of the Franks analysis (whether an allegedly false statement is necessary to a finding of probable cause) is a legal question that we review de novo. Id. (explaining that "conclusions of law are reviewed de novo"). Probable cause exists if the remaining portions of the affidavit provide the court "with a basis for finding that there was a fair probability that contraband or evidence of a crime would be found." Id. at 504. Only if the defendant can make a substantial preliminary showing that specified portions of the affidavit are *deliberately* or *recklessly* false, and, that probable cause would not be supported by the remaining content of the affidavit, then and only then will a hearing be granted (emphasis added). It is important that the standard is not any false statement, but a material, and deliberate or reckless statement.

Popa fails to develop his Franks argument based in large part on the fact that TFO Anschutz's statements in the Affidavit are neither deliberately or recklessly false. Therefore, Popa has failed to meet the first prong of the Franks test to warrant a hearing on this issue.

IV. CONCLUSION

For the reasons stated above, the government hereby respectfully requests that the Court (1) deny the defendant's motion to compel the production of the law enforcement sensitive program, and (2) deny the defendant's motion to suppress as there was sufficient probable cause to authorize the search of Popa's residence and computer devices.

Respectfully submitted,

JUSTIN E. HERDMAN
United States Attorney

By: /s/ Carol M. Skutnik
Carol M. Skutnik (OH: 0059704)
Assistant United States Attorney
United States Court House
801 West Superior Avenue, Suite 400
Cleveland, OH 44113
(216) 622-3785
(216) 522-8355 (facsimile)
Carol.Skutnik@usdoj.gov

CERTIFICATE OF SERVICE

I hereby certify that on this 21st day of February 2019 a copy of the foregoing document was filed electronically. Notice of this filing will be sent to all parties by operation of the Court's electronic filing system. All other parties will be served by regular U.S. Mail. Parties may access this filing through the Court's system.

/s/ Carol M. Skutnik
Carol M. Skutnik
Assistant U.S. Attorney